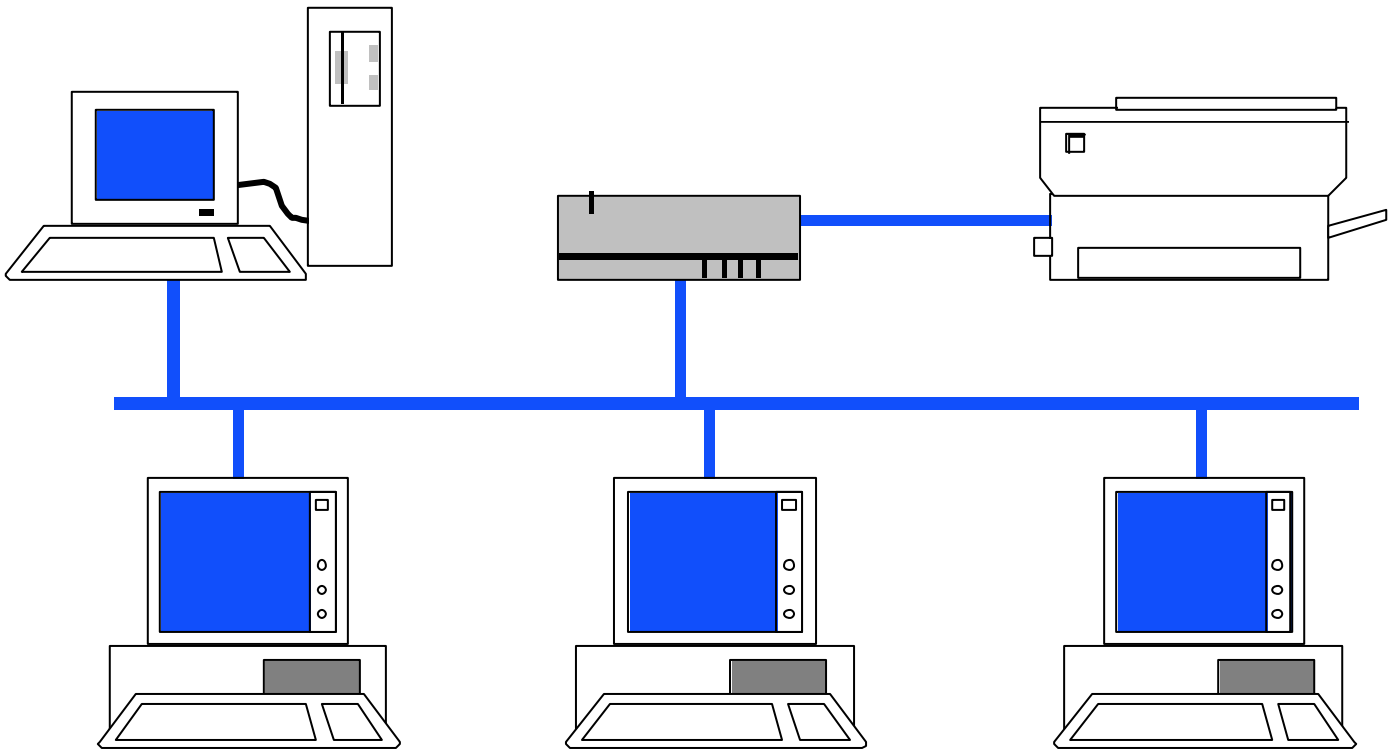
Linux Netzwerke

Mag. Dr. Klaus Coufal



Themenübersicht

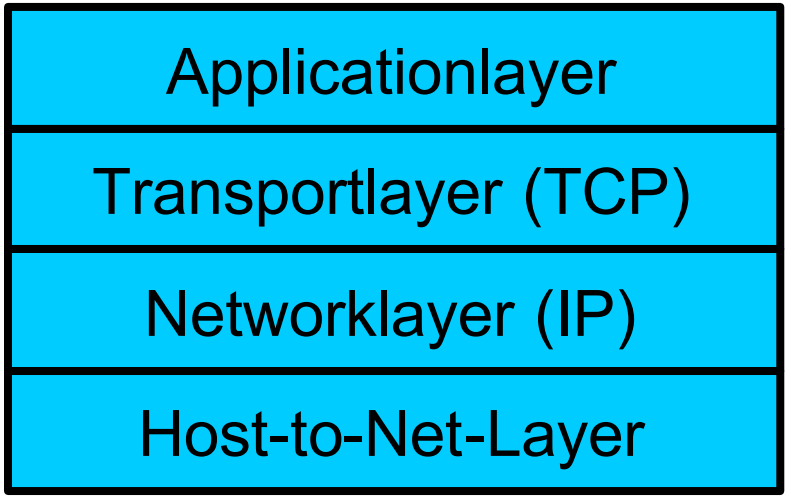
- Linux im Netzwerk
- Anschluß an das Internet
- Wichtige Dienste
- Sicherheit
- Wichtige Kommandos

I. Linux im Netzwerk

- TCP/IP
- IPv4
- IPv6
- Einbindung in das LAN
- Manuelle Konfiguration
- DNS
- DHCP

I.1. TCP/IP

- Im Internet wird ein 4-Schichtenmodell verwendet:



Dabei nimmt TCP die Aufgaben der Transportschicht (Ende-zu-Ende-Kommunikation) und IP die Aufgaben der Netzwerkschicht war

I.2 IPv4

- 32-Bit Adressen mit hierarchischer Struktur und vielen ungenutzen Adressen
- Keine Sicherheit
- Nicht echtzeitfähig (kein QoS)
- Dezimal Schreibweise (z.B.:192.189.51.100)
- Versteckte Adressen
  - 10.x.x.x
  - 172.16.x.x-172.31.x.x
  - 192.168.x.x

IPv4

- Adresse besteht aus Netzanteil und Hostanteil
- Gekennzeichnet durch Netzmaske
- 2 spezielle Adressen
  - Netzadresse (Hostanteil 0)
  - Broadcastadresse (Hostanteil -1)
- Subnetmöglichkeit

I.3. IPv6

- 128-Bit-Adressen
- IPSec integriert
- Echtzeitfähig (durch QoS)
- Kompatibel zu IPv4
- Hexadezimale Schreibweise (z.B.: 3ffe:400:10:abcd:300:c0ff:fed0:5678
- Besser strukturiert

I.4. Einbindung in das LAN

- (Einbau einer Netzwerkkarte)
- Standardkonfiguration mittels Konfigurationswerkzeug der Distribution (YaST2 (SuSE), linuxconf (RedHat))
- Notwendige Parameter:
  - Typ der Netzwerkkarte
  - IP-Address, Netmask, Defaultgateway, IP-Address des/der DNS-Server (oder DHCP)

I.5. Manuelle Konfiguration

- /etc/hosts (address name nickn.)
- /etc/networks (name netaddress)
- /etc/host.conf (Reihenfolge)
- /etc/resolv.conf (DNS-Infos)
- /etc/route.conf (Routinginformationen)
- Systemabhängige weitere (z.B.: /etc/rc.config) Konfigurationsdateien
- Systemspezifische Startskripte

I.6. DNS

- Domain Name Service (Port 53)
- Umwandlung von Rechnernamen in IP-Adresse (z.B.: miraculix.htl-tex.ac.at = 192.189.51.100)
- Hierarchisch aufgebaut (root, tld, sld, ...)
- Rechneranfragen werden beantwortet (eventuell weiterfragen notwendig)

I.7. DHCP

- Dynamic Host Configuration Protocol
- Versuch von zentraler Stelle aus die Netzwerkinformationen (Adresse, Netzmaske, DNS-Server, Gateway) zu verwalten und zu verteilen
- Basis MAC-Adresse
- Relativ großes Sicherheitsrisiko

II. Anschluß an das Internet

- PPP (Point-to-Point-Protocol)
- Internetzugang über ISDN
- Internetzugang über ADSL
- Internetzugang über Kabelmodem

II.1. PPP

- Eigenes Packet
- RFC1144, RFC1321, RFC1332, RFC1334, RFC1548, RFC 1549
- Hat SLIP (Serial Line IP) abgelöst
- Konfiguration über das Konfigurationswerkzeug der Distribution
- (WAN-Interface ist unter ppp0, ppp1, ... verfügbar)

II.2. ISDN-Zugang

- Packet: isdn4linux
- Aktive Karten/Passive Karten
- Konfiguration über das Konfigurationswerkzeug der Distribution
- „Euro-ISDN“
- Notwendig: eigene MSN-Nummer, Provider-ISDN-Nummer, Benutzername, Passwort, DNS-Server

II.3. ADSL-Zugang

- Verwendetes Protokoll: PPPoE (Point-to-Point over Ethernet)
- Parameter in : /etc/pppoed.conf (und eventuell in rc.dialout)
- Dial-on-Demand

II.4. Kabelzugang

- Am einfachsten von allen Internetzugängen in Österreich
- Netzwerkschnittstelle mit dem Anbieter bekannter MAC-Adresse auf DHCP konfigurieren und an das Kabelmodem anschließen
- Fertig

III. Wichtige Dienste

- Samba (Server für Windowsclients)
- Netatalk (Server für MacOS-Clients)
- MARSNWE (Server für NW-Clients)
- FTP (FTP-Server)
- Apache (Webserver)
- Squid (Proxyserver)
- Sendmail (SMTP-Server)
- DNS bzw. DHCP-Server

III.1. Samba

- File-, Print- und Domainserver für DOS-, Windows- und OS/2-Rechner
- Konfig.datei /etc/samba/smb.conf
- SMB-Protocol und NetBIOS-Dienst (NetBEUI)
- Keine Änderung an den Clients notwendig

III.2. Netatalk

- File- und Printserver für MacOS-Rechner
- Konfig.datei /etc/atalk/atalkd.conf
- Implementierung der Apple-Talk-Protokollfamilie
- Keine Änderung an den Clients notwendig

III.3. MARSNWE

- File- und Printserver für Novellclients (DOS, Windows, OS/2, MacOS, ...)
- NDS-Unterstützung noch nicht gut
- Konfig.datei /etc/nwserv.conf
- Implementierung des IPX/SPX und des NCP-Protokolles

III.4. FTP

- Viele Clientvarianten (Commandline, Interaktiv, Graphisch, Webbrowser)
- Aktiv/Passive
- Port 21 (und Port 20)
- Mehrere Serverversionen (wu.ftpd, ...)
- Unsicherer Dienst
- TFTP ohne Authentifizierung

III.5. Apache

- Webserver mit größtem Marktanteil
- Konfig.datei /etc/httpd/httpd.conf
- Verzeichnis unter „ServerRoot“ (z.B.: /usr/local/httpd)
- Dokumente im Unterverzeichnis htdocs
- 1.Datei index.html
- (z.B.: /usr/local/httpd/htdocs/index.html)

III.6. Squid

- Proxyserver für http (Ports 3128, 8080)
- Vorteile eines Proxy-Servers
  - Erhöhung der Performance
  - Erhöhung der Sicherheit
- Nachteile eines Proxy-Servers
  - Performanceverbesserung bei dynamischen Webseiten gering
  - Webverkehr wird bestens überwachbar
- Konfig.datei /etc/squid.conf

III.7. Sendmail

- SMTP-Server (**S**imple **M**ail **T**ransfer **P**rotocol)
- Konfig.datei /etc/sendmail.cf
- In der Tiefe der Möglichkeiten unübersichtlich
- Konfiguration über das Konfigurationswerkzeug der Distribution

III.8. DNS

- Nameserver BIND (derzeit Version 9)
- Konfig.datei /etc/named.conf
- Zusätzlich Zonendateien über verwaltete Domains
- Angabe der Forwarders nötig
- Mindestens 2 Nameserver pro Domäne (einer außerhalb des Netzes)

III.9. DHCP

- Server für DHCP
- Konfig.datei /etc/dhcpd.conf
- Standard: Dynamische Zuordnung aus einem Adresspool
- Fixe Zuordnungen auf Basis der MAC-Adresse möglich
- Zusatzangaben: DNS-Server, Gateway

IV. Sicherheit

- Masquerading (NAT)
- Firewall
- OpenSSH
- Sicherheit generell

IV.1. Masquerading

- Übersetzung von IP-Adressen
- Hauptsächlich bei „versteckten“ Adressen im Einsatz
- z.B.: 192.168.13.2:1199 ⇨ 192.189.51.21:65001
- Dynamisches NAT
- Statisches (Hide)-NAT

IV.2. Firewall

- Sicherheitsmauer zwischen externem und internem Netz
- Realisierung mit ipchains (älter) bzw. iptables
- Packetfiltering (Ansätze zu Statefull Inspection vorhanden, Application Layer Gateway extra realisierbar)
- Konfiguration für Anfänger verwirrend (Vereinfachungen z.B.: SuSEfirewall2, fwbuilder, ...)

IV.3. OpenSSH

- Dieses Packet stellt einen SSH-Server und die Kommandos ssh, scp und sftp zur Verfügung
- Mit asymmetrischen Verfahren verschlüsselte Übertragung
- Ersatz des Passwortes durch Zertifikate möglich

IV.4. Sicherheit generell

- Sicherheit ist ein ständiger Prozeß!
  - Passwörter regelmäßig ändern
  - Logfiles lesen
  - Ständig am neuesten Stand bei sicherheitskritischer Software
- „Feinde“ der Sicherheit:
  - Falsches Vertrauen
  - Bequemlichkeit

V. Wichtige Kommandos

- ifconfig
- route
- netstat
- ping, traceroute
- host, hostname, nslookup, dig
- ssh, scp
- ftp

V.1. ifconfig

- Konfiguriert ein Netzwerkinterface
- Syntax:
  `ifconfig interface [aftype] [options]`

```
root@rechner:/etc > ifconfig eth0
eth0 Link encap:Ethernet  HWaddr 00:00:21:64:3F:B9
     inet addr:192.168.13.1  Bcast:192.168.13.255  Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:11516 errors:0 dropped:0 overruns:0 frame:0
     TX packets:8961 errors:0 dropped:0 overruns:0 carrier:0
     collisions:142 txqueuelen:100
     Interrupt:12 Base address:0xe400
```

V.2. route

- Zeigt und ändert die Routingtabelle
- Syntax: `route [options]`

```
root@rechner:/etc > route -N
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.189.51.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.13.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.189.51.1    0.0.0.0         UG    0      0        0 eth0
```

V.3. netstat

- Zeigt Information über das Netzwerk an
- Syntax: `netstat [options]`

```
root@rechner:/etc > netstat -tunl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address      Foreign Address         State
tcp        0      0 0.0.0.0:22         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21         0.0.0.0:*               LISTEN
```

V.4. ping

- Ping sendet ein Kontrollpacket an eine IP-Adresse und zeigt die Antwort an
- Syntax: `ping [options] host`

```
funk-nat:~ # ping miraculix.htl-tex.ac.at
PING miraculix.htl-tex.ac.at (192.189.51.100) from
   192.189.51.63 : 56(84) bytes of data.
64 bytes from miraculix.htl-tex.ac.at (192.189.51.100):
   icmp_seq=1 ttl=128 time=0.440 ms
funk-nat:~ # ping 192.189.51.1
PING 192.189.51.1 (192.189.51.1) from 192.189.51.63 : 56(84)
   bytes of data.
--- 192.189.51.1 ping statistics ---
3 packets transmitted, 0 received, 100% loss, time 2017ms
```

V.5. traceroute

- Traceroute sucht den Weg zu einem Rechner (mit Hilfe von Pings)
- Syntax: `traceroute [options] host`

```
funk-nat:~ # traceroute www.coufal.info
traceroute to www.coufal.info (62.99.149.13), 30 hops max, 40 byte pkts
 1 sagnix.htl-tex.ac.at (192.189.51.1) 0.136 ms  0.000 ms  0.100 ms
 2 sagnix93.htl-tex.ac.at (193.170.108.1) 7.499 ms  8.377 ms  9.254 ms
 3 Vienna-RBS2.ACO.net (192.153.182.101) 11.175 ms 11.031 ms 11.273 ms
 4 Wien1.ACO.net (193.171.23.1)  10.752 ms  10.990 ms  10.974 ms
 5 interxion.inode.at (193.203.0.57)  10.957 ms   10.949 ms   10.993 ms
 6 l3-suite-C2948G.inode.at (62.99.171.126) 11.037ms 11.064ms 11.109 ms
 7 host5.ssl-gesichert.at (62.99.149.13)  9.644 ms  9.644 ms  9.619 ms
```

V.6. host

- Sucht mit Hilfe eines DNS-Server nach einem Namen
- Syntax: `host [options] host`

```
rechner:~ # host www.htl-tex.ac.at
www.htl-tex.ac.at is a nickname for asterix.htl-tex.ac.at
asterix.htl-tex.ac.at has address 192.189.51.199
rechner:~ # host 192.189.51.199
199.51.189.192.IN-ADDR.ARPA domain name pointer asterix.htl-tex.ac.at
```

V.7. hostname

- Zeigt oder setzt den Netzwerknamen des Systems
- Syntax: `hostname [name]`

```
funk-nat:~ # hostname
funk-nat
```

V.8. nslookup

- Interaktives Hilfsprogramm zum Abfragen eines DNS-Servers
- Syntax: `nslookup [optionen]`

```
firewall:~ # nslookup
Default Server:  ns1.chello.at
Address:  195.34.133.10
> www.coufal.info
Server:  ns1.chello.at
Address:  195.34.133.10

Non-authoritative answer:
Name:    www.coufal.info
Address:  62.99.149.13
> exit
```

V.9. dig

- Hilfsprogramm zum Abfragen eines DNS-Server
- Syntax: `dig domain [options]`

```
firewall:~ # dig www.coufal.org
...

;; ANSWER SECTION:
www.coufal.org.         23h11m56s IN A  62.99.149.10

;; AUTHORITY SECTION:
coufal.org.             23h11m56s IN NS  ns1.domaintechnik.at.
coufal.org.             23h11m56s IN NS  ns2.domaintechnik.at.

...
```

V.10. ssh

- **S**ecure **SH**ell Client (Remote login)
- Syntax: `ssh [-l login_name] [hostname]`

```
funk-nat:~ # ssh cisco.htl-tex.ac.at
root@cisco.htl-tex.ac.at's password:
Last login: Wed Nov 20 17:36:09 2002 from
  ueb05.exp.univie.ac.at
Have a lot of fun...
einsilbix:~ # exit
logout
Connection to cisco.htl-tex.ac.at closed.
```

V.11. scp

- **S**ecure **C**o**P**y (Kopieren von Dateien auf andere Rechner mit Hilfe von SSH)
- Syntax: `scp [options] [[user1]@host1:]file1 [[user2]@host2:]file2`

```
funk-nat:~ # scp root@cisco.htl-tex.ac.at:/tftpboot/Lab_C .
root@cisco.htl-tex.ac.at's password:
Lab_C   100% |*****************************|  1026     00:00
```

V.12. ftp

- Interaktiver Client für FTP-Server
- Syntax: `ftp [options] host [hostoptions]`

```
funk-nat:~ # ftp miraculix.htl-tex.ac.at
Connected to miraculix.htl-tex.ac.at.
220-miraculix.htl-tex.ac.at
220-Welcome at HTBLVA fuer Textilindustrie und Datenverarbeitung
220-
220-Please enter user name with container relativly to EDV.HTBLVA
220-(e.g. PUPIL.HDV, user.ABEND, ...)
220-
220-Your will be connected to your home directory at TALENTIX (R:)!
220-To change to your MIRACULIX-directory use UNC.
220 Service Ready for new User
Name (miraculix.htl-tex.ac.at:root):
```

ftp

Wichtige Befehle:

get file	Hole Datei auf lokalen Rechner
put file	Send Datei von lokalem Rechner
image	Binärmodus zum Übertragen
ascii	ASCII-Modus zum Übertragen
passive	Passiver Modus (pasv)
quit	Aussteigen (auch exit, bye)
help	Hilfe